AMENDMENTS TO THE DRAWINGS

Replacement formal drawings of Figures 1-12 are submitted concurrently herewith under a separate cover letter.

REMARKS

By this Amendment, claims 1-35 are cancelled, and claims 36-55 are added. Thus, claims 36-55 are active in the application. Reexamination and reconsideration of the application are respectfully requested.

The specification and abstract have been carefully reviewed and revised in order to correct grammatical and idiomatic errors in order to aid the Examiner in further consideration of the application. The amendments to the specification and abstract are incorporated in the attached substitute specification and abstract. No new matter has been added.

Also attached hereto is a marked-up version of the substitute specification and abstract illustrating the changes made to the original specification and abstract.

Replacement formal drawings of Figures 1-12 are submitted concurrently herewith under a separate cover letter in order to correct a mislabeled reference numeral. In particular, the reference numeral 110 is used in the specification and in Figures 1-2 to denote the recording medium of the first embodiment of the present invention. Reference numeral 130 is used in the specification and in Figures 1, 3 and 6 to denote the file server 130 of the first embodiment. However, reference numeral 130 was used in Figure 3 to denote both the recording medium and the file server. Accordingly, Figure 3 has been revised to denote the recording medium with reference numeral 110 instead of reference numeral 130. Approval of the replacement formal drawings is respectfully requested.

The Applicants note that the Examiner failed to consider the references listed on the September 14, 2001 Form PTO-1449. The Applicants respectfully request the Examiner to consider the references listed on the September 14, 2001 Form PTO-1449 and to return an Examiner-initialed copy of the September 14, 2001 to the Applicants to indicate consideration of the references listed thereon.

As will be described below, Durham (U.S. Patent Application Publication No. 2005/0010647) was used in the rejection of cancelled claims 1-20. However, the Examiner failed to properly cite Durham on the Form PTO-892 attached to the Office Action. For the Examiner's convenience, a Form PTO-1449 having the Durham reference listed thereon is submitted herewith. The Applicants respectfully request the Examiner to officially cite the Durham reference on a Form PTO-892 or to initial the

Form PTO-1449 having the Durham reference listed thereon in order to formally make the Durham reference of record in the present application.

In item 5 on page 2 of the Office Action, claims 1-4, 6, and 11-14 were rejected under 35 U.S.C. § 102(e) as being anticipated by Durham. In item 11 on page 4 of the Office Action, claims 1-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Durham. Furthermore, in item 14 on page 5 of the Office Action, claims 1-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Durham in view of Wang (U.S. 5,917,913).

These rejections are believed to be moot with respect to claims 1-20 in view of the cancellation of claims 1-20. Furthermore, the Applicants respectfully submit that these rejections are inapplicable to new claims 36-55 for the following reasons.

Conventional computer systems use cookie information for enhancing a computer user's access to a Web site by providing a customized service. The cookie information contains personal information of the user, and the cookie information is stored in the terminal that the user uses to access the Web site. Each time the user access the Web site using the same terminal, the Web site reads the stored cookie information to provide information to the user.

However, since cookie information is stored on the terminal, the cookie information cannot distinguish between several users who use the same terminal. For example, if user A and user B both use the same terminal and access the Web site, the cookie information stored on the terminal contains the personal information of both user A and user B, and thus, the Web site cannot provide a customized service to only the preferences of user A or user B. Furthermore, cookie information may contain sensitive financial or private personal information which may be maliciously used by a third party.

In addition, since cookie information is stored on the terminal that the user used to access the Web site, the user must continue to use the same terminal or must provide his personal information again to the Web site if he uses another terminal.

The present invention provides a method for customizing services that are provided on a network for each user even if several users use the same terminal or different terminals. In particular, the method of the present invention provides that an apparatus on the network reads unique information that is recorded on a transportable

recording medium connected to the apparatus, and customizes the service for each user based on the unique information. The unique information is recorded in an encrypted state and is used after being decrypted by using a media identifier, which is unique to each recording medium. Each user has a recording medium uniquely assigned to him or her.

The present invention thus makes it possible for the apparatus on the network to read the unique information that is recorded on the transportable recording medium, and then customize the service for the user of the recording medium.

Accordingly, if the user uses his own recording medium when the user access a Web site, the relationship between the user and the recording medium becomes one-to-one even if the relationship between the user and the terminal is not one-to-one, i.e., if the user uses a different terminal. Thus, an advantageous effect is achieved whereby the user is able to receive the same customized service even when he uses a different terminal, because the present invention makes it possible for the apparatus and the Web site to handle the correct information for each user.

Further, the present invention provides that the unique information is encrypted and can be decrypted only by using a decryption key which is generated based on a media identifier, which is unique to each recording medium. Accordingly, the present invention provides that it is not possible to decrypt the encrypted unique information if the unique information is copied to a different recording medium, and thus, the encrypted unique information recorded in the different recording medium cannot be used to provide a customized service to the user.

New claim 36 recites a service providing method of providing a current user of a first apparatus with each service provided by a plurality of other apparatuses via a network, where the first apparatus is able to communicate with each of the plurality of other apparatuses via the network and is locally connectable to a recording medium from among recording media that are uniquely assigned to users of the first apparatus, each recording medium has a media identifier as a unique identifier recorded thereon and is transportable, and each recording medium includes an area for storing encrypted unique information which is unique information that has been encrypted.

The method of new claim 36 comprises a service requesting operation of the first apparatus requesting a second apparatus to provide a service desired by the current user, where the second apparatus is one of the plurality of other apparatuses. The method of new claim 36 also comprises a reading operation of, if a recording medium of the current user is locally connected to the first apparatus, the second apparatus reading the unique media identifier in the locally connected recording medium via the first apparatus and the network, and if a recording medium of the current user is locally connected to the first apparatus and stores encrypted unique information, the second apparatus reading the encrypted unique information in the locally connected recording medium via the first apparatus and the network. The method of new claim 36 also comprises a service providing operation of the second apparatus (i) generating a decryption key based on the media identifier read in the reading operation, (ii) generating unique information by decrypting the encrypted unique information read in the reading operation by using the generated decryption key, (iii) customizing the desired service according to the generated unique information, and (iv) transmitting the customized service to the first apparatus.

New claim 46 recites a service providing method used by a first apparatus operable to receive each service provided by a plurality of other apparatuses via a network and provide the received service to a current user of the first apparatus, where the first apparatus is able to communicate with each of the plurality of other apparatuses via the network and is locally connectable to a recording medium from among recording media that are uniquely assigned to users of the first apparatus, each recording medium has a media identifier as a unique identifier recorded thereon and is transportable, and each recording medium includes an area for storing unique information.

The method of new claim 46 comprises a service requesting operation of the first apparatus requesting a second apparatus to provide a service desired by the current user, where the second apparatus is one of the plurality of other apparatuses. The method of new claim 46 also comprises a transmitting operation of, if a recording medium of the current user is locally connected to the first apparatus, the first apparatus reading the unique media identifier in the locally connected recording medium and transmitting the read media identifier to the second apparatus via the network, and if a recording medium of the current user is locally connected to the first apparatus and stores unique

information, the first apparatus reading the unique information in the locally connected recording medium and transmitting the read unique information to the second apparatus via the network. The method of new claim 46 also comprises a service providing operation of the first apparatus receiving a service that has been customized by the second apparatus from the second apparatus and providing the received service to the current user, wherein the second apparatus customizes the customized service by (i) generating a decryption key based on the media identifier that has been transmitted to the second apparatus in said transmitting operation, (ii) generating unique information by decrypting, by using the generated decryption key, the encrypted unique information that has been transmitted to the second apparatus, and (iii) customizing a desired service according to the generated unique information.

Durham discloses a method and apparatus for customizing an options page of a client application at a server instead of requiring the user to customize the options page at the user terminal (client application). In particular, Durham discloses that instead of requiring the user to customize an options page at the user's terminal, the options page is stored at the server, and the server passes the user's current settings to the user through a browser. Durham also discloses that stored cookies may be read from a cookie storage 176 at the user's terminal when the user accesses the server (see paragraphs [0041] and [0051]). Durham, however, merely employs the conventional use of cookies that are stored on a user's terminal, where the cookies are not unique only to the terminal but not to the user himself.

The only similarity between Durham and the inventions of new claims 36 and 46 is the use of information that is assigned to each user, such as cookie information. Otherwise, Durham and new claims 36 and 46 are markedly different.

In particular, as described above, new claims 36 and 46 each recite that the first apparatus (e.g., user terminal) is locally connectable to a recording medium from among recording media that are uniquely assigned to users of the first apparatus, where each recording medium has a media identifier as a unique identifier recorded thereon. However, Durham merely uses cookie information that is stored in the user's terminal to assist in providing a customized Web site to the user's terminal. In fact, Durham does not even contemplate the use of a media identifier which is unique to a portable recording

medium and which is stored on the recording medium. Durham, however, does not even contemplate that the second apparatus (Web site or server) reads the unique media identifier in the locally connected recording medium only if a recording medium of the current user is locally connected to the first apparatus, as recited in new claim 36. Moreover, Durham does not disclose or suggest that the second apparatus reads the encrypted unique information in the locally connected recording medium if a recording medium of the current user is locally connected to the first apparatus and stores encrypted unique information, as recited in new claim 36.

Similarly, Durham does not disclose or suggest a transmitting operation of, if a recording medium of the current user is locally connected to the first apparatus, the first apparatus reading the unique media identifier in the locally connected recording medium and transmitting the read media identifier to the second apparatus via the network, and if a recording medium of the current user is locally connected to the first apparatus and stores unique information, the first apparatus reading the unique information in the locally connected recording medium and transmitting the read unique information to the second apparatus via the network, as recited in new claim 46.

Furthermore, Durham clearly does not disclose or suggest a service providing operation of the second apparatus (i) generating a decryption key based on the media identifier read in the reading operation, (ii) generating unique information by decrypting the encrypted unique information read in the reading operation by using the generated decryption key, (iii) customizing the desired service according to the generated unique information, and (iv) transmitting the customized service to the first apparatus, as recited in new claim 36.

Similarly, Durham clearly does not disclose or suggest a service providing operation where the second apparatus customizes a service by (i) generating a decryption key based on the media identifier that has been transmitted to the second apparatus in said transmitting operation, (ii) generating unique information by decrypting, by using the generated decryption key, the encrypted unique information that has been transmitted to the second apparatus, and (iii) customizing a desired service according to the generated unique information, as recited in new claim 46.

Accordingly, Durham clearly does not disclose or suggest each and every limitation of new claims 36 and 46. Therefore, new claims 36 and 46 are not anticipated by Durham since Durham clearly fails to disclose each and every limitation of new claims 36 and 46.

Furthermore, for the following reasons, the addition of Wang does not cure the deficiencies of Durham for failing to disclose or suggest each and every limitation of new claims 36 and 46

Wang discloses a portable electronic authorization device for approving a transaction request which has originated from an electronic transaction system, where user information may be encrypted to signify approval of the transaction by the user (see Column 2, line 66 to Column 3, line 28, and Column 11, lines 33-49).

Wang and the inventions of new claims 36 and 46 are similar in that the information about the user is securely recorded and that the information about the user is encrypted when the information is transmitted. However, the similarities between Wang and new claims 36 and 46 end there.

In particular, in Wang, the information that is recorded on the recording medium is not encrypted, and the information is encrypted only when it is transmitted. However, new claims 36 and 46 each recite that unique information is recorded in the encrypted state, whereby the unique information does not need to be encrypted each time the information is transmitted. Furthermore, in Wang, the information is encrypted by using the public key. However, as recited in each of new claims 36 and 46, the information is encrypted by using the media identifier which is unique to the recording medium.

Moreover, in Wang, it is essential to record the information in the secure area because the information is recorded without being encrypted. However, in the inventions of new claims 36 and 46, it is not necessary to record the information in the secure area because the information is recorded in the encrypted state, even though the media identifier is recorded in the secure area. Therefore, according to the inventions of new claims 36 and 46, it is possible to increase security when the information is recorded in the secure area, and it is possible to obtain both high security and convenience when the information is recorded in the non-secure area of the user's recording medium.

Furthermore, as described above, the unique information is encrypted by using the media identifier which is unique to the user's portable recording medium. Therefore, if someone tries to use the encrypted unique information that is recorded in a different recording medium on the same terminal, it is not possible to decrypt the encrypted unique information because the media identifier is different, which renders the encrypted unique information unusable if the proper recording medium is not used. Neither Durham nor Wang disclose this advantageous effect of new claims 36 and 46.

Furthermore, neither Durham nor Wang disclose, suggest or even contemplate the use of a media identifier which is unique to each portable recording medium. Therefore, it could not have been possible to conceive of the methods of new claims 36 and 46 from the disclosure of Durham and Wang, either individually or in combination, since Durham and Wang do not even contemplate the use of a unique media identifier in decrypting encrypted unique information.

Accordingly, for at least the foregoing reasons, new claims 36 and 46 are clearly patentable over Durham and Wang since Durham and Wang, either individually or in combination, clearly fail to disclose or suggest each and every limitation of new claims 36 and 46.

The Examiner alleged that "it would have been obvious...to use unique device or media identifiers...for the purpose of authentication or identification of such device or media." Although the Examiner provided no support for this conclusory assertion, even if this assertion was correct, it would not render new claims 36 and 46 unpatentable. New claims 36 and 46 each recite that the media identifier is used for decrypting the information recorded on the recorded medium, and not for "the purposes of authentication or identification of such device or media."

That is, even if the Examiner contends that using a unique media identifier of the recording medium for "authentication or identification of such device or media" is obvious, using the media to generate a decryption key and generate unique information by decrypting the encrypted unique information recorded on the recording medium, as recited in new claims 36 and 46, is clearly not obvious. New claims 36 and 46 each provide the above-described unique and advantageous effect that could not have been

obtained if the media identifier was used merely for user verification or authentication of the device or media.

Accordingly, for at least the foregoing reasons, new claims 36 and 46 are clearly patentable over Durham and Wang since Durham and Wang, either individually or in combination, clearly fail to disclose, suggest or even contemplate each and every limitation of new claims 36 and 46.

Furthermore, it is submitted that the clear distinctions discussed above are such that a person having ordinary skill in the art at the time the invention was made would not have been motivated to modify Durham and Wang in such as manner as to result in, or otherwise render obvious, the present invention as recited in new claims 36 and 46. Therefore, it is submitted that the new claims 36 and 46, as well as new claims 37-45 and 47-55 which depend therefrom, are clearly allowable over the prior art as applied by the Examiner.

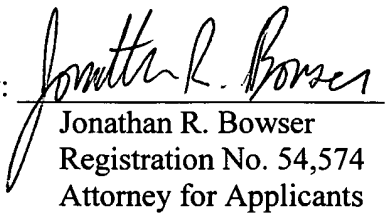
In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. An early notice thereof is respectfully solicited.

If, after reviewing this Amendment, the Examiner feels there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

A fee and a Petition for a one-month Extension of Time are filed herewith pursuant to 37 CFR § 1.136(a).

Respectfully submitted,

Hideki MATSUSHIMA et al.

By: 

Jonathan R. Bowser
Registration No. 54,574
Attorney for Applicants

JRB/nrj
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
August 18, 2005

Version with Markings to Show Changes Made

~~TITLE OF THE INVENTION~~

SERVICE PROVIDING APPARATUS AND METHOD THAT ALLOW AN APPARATUS TO ACCESS QNIQUE INFORMATION STORED IN TRANSPORTABLE RECORDING MEDIUM

This Application is a continuation-in-part under 35 U.S.C. § 120 of U.S. application Serial No. 09/402,521, filed January 14, 2000, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to data communication between a user's apparatus and another apparatus, such as the access from a terminal on the Internet to a Web site. More particularly, the present invention relates to a technique of facilitating the handling of personal information of each user and enhancing the security of the personal information.

2. Description of the Related Art

In recent years, the Internet has become increasingly popular, and more and more services are being provided on the Internet. A major service offered on the Internet is ~~WWW~~ the ~~(~~World Wide Web~~)~~ (WWW), which ~~that~~ is a client/server-type information search system. In the WWW, server apparatuses (Web sites) provide information in HTML files and users of the Internet browse the information using browsing software called Web browsers at terminals (Web clients) Various information and services are currently provided at numerous Web sites, and a technology called "cookies" is widely used to provide information with efficiency. When a user enters a Web site) the Web site stores data, such as personal information of the user, as a cookie in the terminal of the user through the Web browser. The next time the user goes to the same Web site using the same terminal, the Web site reads the cookie from the terminal and uses the read cookie to provide information to the user.

Cookies usually show personal information of users, the last dates and times the users visited Web sites, and the numbers of times the users have visited the Web sites. Cookies are also used to identify users. Therefore, cookies are used as an element of technology in various. authentication systems and personalizing systems that customize services provided in the WWW for respective users and provide the customized services to the users.

While being a useful technology, cookies also have the following problems. ~~described below.~~ One problem is ~~caused by~~ that Web sites store data, such as personal information of users, into terminals with which the users visit the Web sites. If a single user uses a plurality of terminals or a plurality of users shares a single terminal or a plurality of terminals, ~~therefore,~~ Web sites cannot correctly obtain and use information of respective users with cookies. Also, if a user replaces an old terminal with new one, data stored as a cookie in the old terminal does not exist in the new terminal. Therefore, to continuously use the cookie even after the replacement of the terminal, the user needs to copy the cookie from the old terminal to the new terminal, which constitutes a burden on the user.

Another problem is ~~caused by~~ that personal information of users may be automatically stored as cookies without the users intending to do so, and even other Web sites, which are not the sites that stored cookies, may refer to the cookies with relative ease. Consequently, there may be cases where cookies are maliciously read, causing user's privacy to be violated or making users a victim of cyber fraud. This generates demand for the enhancement of the security of personal information.

SUMMARY OF THE INVENTION

The object of the present invention is therefore to provide a service providing apparatus, a service providing method, and a service providing program for use with a technology, such as cookies, that customizes services which are provided via a network for respective users. Each of the service providing apparatus, the service providing method, and the service providing program correctly handles information which is unique to each user even if a single user uses a plurality of terminals or a plurality of users shares a single terminal or a plurality of terminals. Each of the service providing apparatus, the

service providing method, and the service providing program also eliminates the need for users to perform burdensome operations, such as the copy of data, even if the users replace old apparatuses with new ones. Each of the service providing apparatus, the service providing method, and the service providing program further enhances the security of personal information. The object of the present invention is also to provide a recording medium that stores the service providing program and a recording medium that stores cookie information.

The stated object is achieved by a service providing method of providing a current user of a first apparatus with each of the services that are provided by a plurality of other apparatuses via a network, where the first apparatus ~~being~~ is able to communicate with each of the plurality of other apparatuses via the network and ~~being~~ is locally connectable to a recording medium~~, out of~~ from among recording media that are uniquely assigned to users of the first apparatus, and each recording medium ~~being~~ is transportable and ~~including~~ includes an area for storing unique information~~, the~~. The service providing method ~~including~~includes: a service requesting step where the first apparatus requests a second apparatus to provide a service that is desired by the current user, the second apparatus being one of the plurality of other apparatuses; a unique information reading step where. if a recording medium of the current user is locally connected to the first apparatus and stores unique information, the second apparatus reads the unique information in the locally connected recording medium via the first apparatus and the network; and a service providing step where the second apparatus customizes the desired service according to the read unique information and transmits the customized service to the first apparatus.

With this method, an apparatus on the network reads the unique information stored in a transportable recording medium and customizes a service according to the read unique information.

Also, if users are uniquely provided with recording media, the users are in a one-to-one correspondence with the recording media even if the users are not in a one-to-one correspondence with terminals. Therefore, when a user browses a Web site, personal information of the user is correctly obtained from the user's recording medium. Also,

even after replacing an old terminal with a new one, the user can continuously receive the same service by simply connecting the user's recording medium to the new terminal.

Here, in the unique information reading step, if ~~no~~ unique information is not stored in the locally connected recording medium or ~~no~~ a recording medium is not locally connected to the first apparatus, the second apparatus may not read unique information from anywhere~~, and~~. Furthermore, in the service providing step, if no unique information has been read in the unique information reading step, the second apparatus may transmit the desired service to the first apparatus in an uncustomized state.

With this method, if the unique information is not read, the apparatus provides the user with a service that is not customized.

This allows the user to receive a service even without unique information. Also, because the unique information is stored only in the recording medium, the security of the unique information is enhanced.

Here, the unique information stored in each recording medium may include user information that is inherent ~~in~~ to a user which is assigned the recording medium, and in the service providing step, the second apparatus may customize the desired service for the current user according to the user information that is included in the read unique information and transmit the customized service to the first apparatus.

With this method, the apparatus reads user information included in the unique information stored in the transportable recording medium and customizes the service for the user according to the user information.

Also, because the user information is stored in the transportable recording medium, the user can continuously use the same personal information without difficulty, even after replacing an old terminal with a new one.

Here, the service providing method may further include: a user information updating step, which is performed after the unique information reading step, where if the user information that is inherent ~~in~~ to the current user needs to be updated, the second apparatus updates the user information that is included in the read unique information and overwrites the user information in the locally connected recording medium with the updated user information via the network and the first apparatus.

With this method, if the user information needs to be updated, the second apparatus updates the user information. This makes it easy to manage the user information.

Here, the user information in each recording medium may have been encrypted by using a public key of a public key cryptosystem, the second apparatus may store a secret key corresponding to the public key, the second apparatus may decrypt the encrypted user information by using the secret key and customize the desired service according to the decrypted user information in the service providing step, and the second apparatus may update the decrypted user information, encrypt the updated user information by using the public key, and overwrite the encrypted user information in the locally connected recording medium with the updated and encrypted user information in the user information updating step.

With this method, user information that has been encrypted by using a public key is transmitted and received. As a result, the encrypted user information is read only by an authorized apparatus that stores a secret key.

Here, the network may be the Internet, the first apparatus may be an Internet terminal that runs a specialized Internet browser, each of the plurality of other apparatuses maybe a Web site, the unique information stored in each recording medium may include cookie information that is used through the Internet browser, and each recording medium may store the cookie information as a file.

With this method, cookie information that has conventionally been recorded on a hard disc is stored in a transportable recording medium.

This reduces the possibility that the cookie information maybe maliciously read, ~~causing~~ which would cause a user's privacy to be violated or ~~making~~ make the user a victim of cyber fraud.

Here, the unique information stored in each recording medium may include a media identifier of the recording medium, the second. apparatus may store user information so that user information that is inherent ~~in~~ to each user is associated with the media identifier of the recording medium assigned to the user, and the service providing step may include: a user information finding substep where the second apparatus finds user information associated with the media identifier included in the read unique

information; and a customizing substep where the second apparatus customizes the desired service for the current user according to the found user information.

This allows the second apparatus to search for user information corresponding to the media identifier included in the unique information that is stored in the transportable recording medium and to customize the service for the user according to the user information.

~~Even~~ Therefore, even after replacing an old terminal with a new one, ~~therefore,~~ the user can continuously receive the same service with the recording medium that is uniquely assigned to the user. Also, because the user information does not reside in the user's terminal, the possibility is reduced that the user information may be maliciously read from the user's terminal, ~~causing~~ which would cause a user's privacy to be violated or ~~making~~ make the user a victim of cyber fraud.

Here, the service providing method may further include: a recording medium connection step, which is performed before the service requesting step, where the first apparatus is locally connected to the recording medium that is assigned to the current user.

With this method, the recording medium is uniquely assigned to the user of the first apparatus and is locally connected to the first apparatus.

Because the user uses the uniquely assigned recording medium, personal information is correctly obtained for the user.

Here, the unique information stored in each recording medium may include a media identifier of the recording medium and user information that is inherent ~~in~~ to a user which is assigned the recording medium, where the user information ~~having~~ has been encrypted~~, and~~. Furthermore, the service providing step may include: a user password receiving substep where the second apparatus receives a user password from the current user via the first apparatus; a decryption key generating substep where the second apparatus generates a decryption key from the media identifier that is included in the read unique information and the received user password; a decryption substep where the second apparatus decrypts the encrypted user information that is included in the read unique information by using the generated decryption key; and a customizing substep

where the second apparatus customizes the desired service for the current user according to the decrypted user information.

With this method, the encrypted user information is decrypted by using the decryption key generated from the media identifier and the user password. This enhances the security of the user information.

Here, each recording medium may include a secure data area, the. media identifier of each recording. medium may be stored in the secure data area of the recording medium~~, and~~. Furthermore, the unique information reading step may include: a device authentication substep where a device authentication is performed between the first apparatus and the locally connected recording medium; and a reading prohibition substep where, if the device authentication has ended in failure, the second apparatus is prohibited ~~to read~~from reading data from the secure data area of the locally connected recording medium.

With this method, if the device authentication has ended in failure, the media identifier is not read. This enhances the security of the user information.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects, advantages and features of the present invention will become more apparent from the following detailed description ~~thereof~~ when taken in conjunction with the accompanying drawings which illustrate ~~a~~ specific embodiments of the present invention. In the drawings:

FIG. 1 shows the construction of an information processing system of the first embodiment of the present invention;

FIG. 2 shows the detailed construction of a recording medium;

FIG. 3 shows the construction of an information processing apparatus;

FIG. 4 shows an example of the content of personal information that is written by a writing unit into a non-secure data area of the recording medium;

FIG. 5 shows the construction of a file server;

FIG. 6 is a flowchart showing the processing procedure of the information processing system of the first embodiment;

FIG. 7 shows the construction of an information processing system of the second embodiment of the present invention;

FIG. 8 shows the detailed construction of a recording medium;

FIG. 9 shows the construction of an information processing apparatus;

FIG. 10 shows the construction of a file server;

FIG. 11 shows an example of the content of the personal information that is stored in a storing unit; and

FIG. 12 is a flowchart showing the processing procedure of the information processing system of the second embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

<First Embodiment>

<Overview>

In an information processing system 100 of the first embodiment of the present invention, the data area for storing cookies is reserved in a transportable recording medium. This allows the cookies to be used in different terminals by simply connecting the transportable recording medium to the respective terminals. This also ~~has~~ allows cookies, which ~~has~~ have conventionally been unique to respective terminals, become unique to respective users.

The recording medium includes a secure data area that stores a media identifier and is accessible only by terminals whose authenticities have been ~~proved~~ proven by the device authentication with the recording medium. The recording medium also includes a data area that is not secure and stores a cookie, such as user information, that has been encrypted by using a public key that is obtained under a public key cryptosystem. It should be noted here that the data area that is not secure is hereinafter referred to as the "non-secure data area".

A Web site which is requested by an authorized terminal to provide a service reads the media identifier from the secure data area via the terminal, and identifies the user of the terminal by using the read media identifier. The Web site also reads the encrypted cookie from the non-secure data area, decrypts the read cookie by using a

secret key stored in the Web site, customizes the service according to the decrypted cookie, and provides the customized service to the terminal.

It should be noted here that if the device authentication between the recording medium and the terminal has ended in failure, the media identifier is not read and the Web site cannot identify the user.

Also, unauthorized Web sites do not store the secret key, ~~so that~~and as a result, the encrypted cookie cannot be decrypted by the unauthorized Web sites. ~~As a result~~Therefore, the security of personal information is enhanced ~~in comparison with~~as compared to a conventional system.

<Construction>

FIG. 1 shows the construction of the information processing system 100 of the first embodiment.

The information processing system 100 includes a recording medium 110, an information processing apparatus 120, and a file server 130.

The recording medium 110 is, for instance, a semiconductor medium, such as a memory card, and a user locally connects the recording medium 110 to the information processing apparatus 120 via a port, a slot, or the like.

The information processing apparatus 120 is a client apparatus, such as an Internet terminal, that runs a specialized Web browser and is connected to a network, such as the Internet. The information processing apparatus 120 is connected to the file server. 130 via the network, issues an access request to the file server 130, and browses information that is provided in HTML files by the file server 130.

The file server 130 is a server apparatus, such as a Web site, that is connected to a network, such as the Internet. The file server 130 is connected to the information processing apparatus 120 via the network and provides information in the form of HTML files to the information processing apparatus 120.

It should be noted here that the information processing apparatus 120 is not limited to an Internet terminal and may be any other device that cat access the information provided by the file server 130 via the network. For instance, the information

processing apparatus 120 may be an Internet-accessible TV, a STB (set top box), a radio cassette tape recorder, a microwave oven, or a refrigerator.

FIG. 2 shows the detailed construction of the recording medium 110.

As shown in ~~this drawing~~FIG. 2, the recording medium 110 includes a secure data area 111, a non-secure data area 112, and an authentication unit 113. A media ID is stored in the secure data area 111.

It should be noted here that media IDs are identifiers which are unique to respective recording media, and the media IDs are used to identify users and to generate encryption keys.

The authentication unit 113 performs an existing device. authentication, such as a mutual authentication, with an apparatus to which the recording medium 110 is connected. In this first embodiment, the authentication unit 113 performs a mutual authentication with an authentication unit 124 of the information processing apparatus 120.

The secure data area 111 is a storage area that cannot be accessed without an access right. That is, the information processing apparatus 120 can access the secure data area 111 only if the device authentication between the recording medium 110 and the information processing apparatus 120 has succeeded~~, the information processing apparatus 120 can access the secure data area 111.~~.

The non-secure data area 112 is a storage area that can be freely accessed. That is, the information processing apparatus 120 can access the non-secure data area 112 even if the device authentication between the recording medium 110 and the information processing apparatus 120 has ended in failure.

FIG. 3 shows the construction of the information processing apparatus 120.

As shown in ~~this drawing~~FIG. 3, the information processing apparatus 120 includes an input unit 121, an encryption unit 122, a transmission unit 123, an authentication unit 124, a receiving unit 125, a reading unit 126, a display unit 127, and a writing unit 128.

The input unit 121 is an input device, such as a combination of a mouse and a keyboard, and receives various inputs from a user. In this first embodiment, the input unit 121 receives a service providing request and personal information. from the user. Here,

the service providing request is a request for providing a service. Also, the personal information is information which is unique to the user, such as the user's name, age, date of birth, sex, family, hobby, taste, address, telephone number, job, E-mail address, credit card number, and password.

The encryption unit 122 encrypts the personal information received by the input unit 121. Here, the encryption unit 122 receives a public key that has been obtained under a public key cryptosystem, such as a RSA cryptosystem, from the file server 130 and prestores the public key. The encryption unit 122 encrypts the personal information by using the public key.

The transmission unit 123 transmits, to the file server 130, the service providing request received by the input unit 121, the media ID read by the reading unit 126, the personal information encrypted by the encryption unit 122, and the encrypted personal information read by the reading unit 126. Here, if the reading unit 126 ~~reads no~~does not read personal information, the transmission unit 123 transmits a personal information unregistered notification, instead of the personal information. The personal information unregistered notification is a notification showing that no personal information has been read. The authentication unit 124 performs an existing device authentication, such as a mutual authentication, with a recording medium that is connected to the information processing apparatus 120.

In this first embodiment, the authentication unit 124 performs a mutual authentication with the authentication unit 113 of the recording medium 110.

The receiving unit 125 receives, from the file server 130, a media ID transmission request, a personal information transmission request, a service file, data for a personal information registration screen, and encrypted personal information. Here, the media ID transmission request is a request for transmitting the media ID, and the personal information transmission request is a request for transmitting the personal information. Also, the personal information registration screen is a screen for allowing the user to register personal information. Further, in addition to the information items of the personal information received by the input unit 121, the personal information received by the receiving unit 125 includes information concerning the Web site (the file server 130), such as the last date and time the user visited the Web site and the number of times the

user has visited the Web site. The service file contains screen data which is provided as part of the service that the user requested by issuing the service providing request. The screen data is, for instance, used to display various information screens or a screen explaining an operating procedure.

The reading unit 126 reads, if a media ID transmission request is received by the receiving unit 125, the media ID from the secure data area 111 of the recording medium 110. Also, if a personal information transmission request is received by the receiving unit 125, the reading unit 126 reads the personal information from the non-secure data area 112 of the recording medium 110. It should be noted here that if the device authentication between the recording medium 110 and the information processing apparatus 120 has ended in failure, the access to the secure data area 111 is prohibited so that the reading unit 126 cannot read the media ID from the secure data area 111.

The display unit 127 displays a personal information registration screen according to the data for the personal information registration screen that is received by the receiving unit 125. The display unit 127 also displays a service screen for the user according to the service file that is received by the receiving unit 125. The service screen is a screen which is displayed as part of the service that the user requested by issuing the service providing request.

The writing unit 128 writes encrypted personal information, which have been received ~~and encrypted~~ by the receiving unit 125, into the non-secure data area 112 of the recording medium 110.

FIG. 4 shows an example of the content of the personal information that is written by the writing unit 128 into the non-secure data area 112 of the recording medium 110.

FIG. 5 shows the construction of the file server 130.

As shown in ~~this drawing~~FIG. 5, the file server 130 includes a receiving unit 131, a user identifying unit 132, a decryption unit 133, a file material storing unit 134, a file editing unit 135, a personal information updating unit 136, and a transmission unit 137.

The receiving unit 131 receives a service providing request, a media ID, ~~an~~ encrypted personal information, a personal information unregistered notification, and a personal information changing request from the transmission unit 123 of the information

processing apparatus 120. The personal information changing request is a request for changing the personal information.

The user identifying unit 132 identifies the user by using the media ID received by the receiving unit 131.

The decryption unit 133 decrypts the encrypted personal information that is received by the receiving unit 131. Here, the decryption unit 133 prestores a secret key that has been obtained under a public key cryptosystem, such as a RSA cryptosystem, and decrypts the encrypted personal information by using the secret key.

The file material storing unit 134 stores file materials that have been classified according to hobbies and tastes of users.

The file editing unit 135 refers to the personal information that is decrypted by the decryption unit 133, and generates a service file by extracting each file material, which corresponds to the user's hobby and taste shown by the decrypted personal information, from the file material storing unit 134 and editing each extracted file material.

The personal information updating unit 136 provides the data for the personal information registration screen, updates the personal information that is decrypted by the decryption unit 133, and encrypts the updated personal information, if the receiving unit receives a personal information unregistered notification or a personal information changing request. Here, the personal information updating unit 136 prestores a public key that has been obtained under a public key cryptosystem, such as a RSA cryptosystem, updates the personal information by changing information concerning the Web site, such as the last date and time the user visited the Web site and the number of times the user has visited the Web site, and encrypts the updated personal information by using the public key.

The transmission unit 137 transmits a media ID transmission request and a personal information transmission request if the receiving unit 131 receives a service providing request. The transmission unit 137 also transmits the service file generated by the file editing unit 135, the data for the personal information registration screen provided by the personal information updating unit. 136, and the personal information that has been updated and encrypted by the personal information updating unit 136.

<Operation >

FIG. 6 is a flowchart showing the processing procedure of the information processing system 100 of the first embodiment.

The processing procedure is briefly described below with reference to ~~this drawing~~FIG. 6.

(1) The input unit 121 of the information processing apparatus 120 receives a service providing request from the user (step S1).

(2) The transmission unit 123 of the information processing apparatus 120 transmits the service providing request received by the input unit 121 to the file server 130 (step S2).

(3) The receiving unit 131 of the file server 130 receives the service providing request from the information processing apparatus 120 (step S3).

(4) The transmission unit 137 of the file server 130 transmits a media ID transmission request and a personal information transmission request to the information processing apparatus 120 (step S4)

(5) The receiving unit 125 of the information processing apparatus 120 receives the media ID transmission request and the personal information transmission request from the file server 130 (step S5).

(6) The reading unit 126 reads a media ID from the secure data area 111 of the recording medium 110 according to the media ID transmission request. Also, the reading unit 126 reads encrypted personal information from the non-secure data area 112 of the recording medium 110 according to the personal information transmission request. Needless to say, if no personal information is stored in the non-secure data area 112, the reading unit 126 cannot read personal information from the non-secure data area 112 (step S6).

(7) The transmission unit 123 of the information processing apparatus 120 transmits the media ID and the encrypted personal information read by the reading unit 126 to the file server 130. If the reading unit 126 has not read ~~no~~ personal information, the transmission unit 123 transmits a personal information unregistered notification, instead of personal information (step S7).

(8) The receiving unit 131 of the file server 130 receives a pair of the media ID and the encrypted personal information or a pair of the media ID and the personal information unregistered notification. The user identifying unit 132 identifies the user by using the received media ID (step S8).

(9) It is judged whether the receiving unit 131 has received personal information or a personal information unregistered notification (step S9).

(10) If the receiving unit 131 has received a personal information unregistered notification, the personal information updating unit 136 provides the data for the personal information registration screen and the transmission unit 137 transmits the provided data (step S10).

(11) The receiving unit 125 of the information processing apparatus 120 receives the data for the personal information registration screen that is transmitted from the file server 130, and the display unit 127 displays the personal. information registration screen (step S11).

(12) The input unit 121 receives personal information inputted by the user through the personal information registration screen (step S12).

(13) The encryption unit 122 encrypts the personal information received by the input unit 121, and the transmission unit 123 transmits the encrypted personal information to the file server 130 (step S13).

(14) The receiving unit 131 of the file server 130 receives the encrypted personal information (step S14).

(15) The decryption unit 133 decrypts the encrypted personal information received by the receiving unit 131 (step S15).

(16) The file editing unit 135 refers to the personal information that is decrypted by the decryption unit 133, and generates a service file by extracting each file material, which corresponds to the user's hobby and taste shown by the decrypted personal information, from the file material storing unit 134 and editing each extracted file material (step S16).

(17) The personal information updating unit 136 updates the personal information that is decrypted by the decryption unit 133 and encrypts the updated personal information (step S17).

(18) The transmission unit 137 transmits the service file generated by the file editing unit 135 and the personal information that is updated and encrypted by the personal information. updating unit 136 (step S18).

(19) The receiving unit 125 of the information processing apparatus 120 receives the service file from the file server 130, and the display unit 127 display a service screen for the user according to the received service file. The receiving unit 125 also receives the updated and encrypted personal information, and the writing unit 128 writes the received personal information into the non-secure data area 112 of the recording medium 110 (step S19).

As described above, in the information processing system of the first embodiment, personal information concerning a user is encrypted and stored in a transportable recording medium, and a server reads the personal information from the recording medium, decrypts the read personal information, and customizes a requested service for the user according to the decrypted personal information. To use an information processing apparatus, each user needs to connect a transportable recording medium, which is uniquely assigned to the user and stores personal information of the user, to the information processing apparatus. This allows the file server to correctly handle personal information of each user. In the information processing system of the first embodiment, the security of personal information is also enhanced because personal information that has been encrypted is stored in a transportable recording medium.

It should be noted here that an encryption key may be generated from a media ID, and personal information may be encrypted by using the encryption key and stored in the non-secure data area of a recording medium. Also, an encryption key may be generated from a media ID and a user password designated by a user.

In the first embodiment, encrypted personal information concerning a user is stored in the non-secure data area of a transportable recording medium. However, the encrypted personal information may be stored in the secure data area of the transportable recording medium. In this case, the recording medium does not need to include a non-secure data area.

If a recording medium is not connected to the information processing apparatus or if a recording medium connected to the information processing apparatus ~~stores no~~does

not store personal information, the file server may provide a requested service without customizing the service.

<Second Embodiment >

<Overview >

In the first embodiment, encrypted personal information concerning a user is stored in a transportable recording medium. In the second embodiment, however, personal information that is not encrypted is stored in a file server.

In this second embodiment, each transportable recording medium stores a media identifier and is uniquely provided to a user. A file server stores personal information of respective users, with the personal information of each user being associated with one media identifier. The file server reads a media identifier from a recording medium, searches for personal information corresponding to the media identifier, and customizes a service according to the corresponding personal information.

In the first embodiment, encrypted personal information is stored and transmitted to enhance the security of personal information. In the second embodiment, although encrypted personal information is transmitted between the information processing apparatus and the file server ~~like~~ similar to the first embodiment, personal information that is not encrypted is stored in a file server. This is because there is no security problem in the file server.

<Construction >

FIG. 7 shows the construction of an information processing system 200 of the second embodiment.

As shown in ~~this drawing~~FIG. 7, the information processing system 200 includes a recording medium 210, an information processing apparatus 220, and a file server 230.

The recording medium 210, the information processing apparatus 220, and the file server 230 are respectively similar to the recording medium 110, the information processing apparatus 120, and the file server 130.

The construction elements having the same functions as those of the first embodiment are assigned the same names and ~~numbers~~ reference numerals as in the first embodiment and are not described here.

FIG. 8 shows the detailed construction of the recording medium 210.

As shown in ~~this drawing~~FIG. 8, the recording medium 210 includes a secure data area 111, a non-secure data area 112, and an authentication unit 113. A media ID is stored in the secure data area 111.

FIG. 9 shows the construction of the information processing apparatus 220.

As shown in ~~this drawing~~FIG. 9, the information processing apparatus 220 includes an input unit 121, an encryption unit 122, a transmission unit 223, an authentication unit 124, a receiving unit 225, a reading unit 226, and a display unit 127.

The transmission unit 223 transmits the service providing request received by the input unit 121, the media ID read by the reading unit 226, and the personal information encrypted by the encryption unit 122 to the file server 230. Here, if the reading unit 226 cannot read a media ID, the transmission unit 223 transmits a media ID reading impossible notification, instead of the media ID. The media ID reading impossible notification is a notification showing that the reading unit 226 has not read ~~no~~ a media ID.

The receiving unit 225 receives a media ID transmission request, a service file, and data for a personal information registration screen from the file server 230.

The reading unit 226 reads, if a media ID transmission request is received by the receiving unit 225, a media ID from the secure data area 111 of the recording medium 210. It should be noted here that if the device authentication between the recording medium 210 and the information processing apparatus 220 has ended in failure, the access to the secure data area 111 is prohibited so that the reading unit 226 cannot read the media ID from the secure data area 111.

FIG. 10 shows the construction of the file server 230.

As shown ~~this drawing~~in FIG. 10, the file server 230 includes a receiving unit 231, a personal information searching unit 232, a decryption unit 133, a file material storing unit 134, a file editing unit 235, a personal information updating unit 236, a transmission unit 237, and a storing unit 238.

The receiving unit 231 receives a service providing request, a media ID, encrypted personal information, a media ID reading impossible notification, and a personal information changing request from the transmission unit 223 of the information processing apparatus 220.

The personal information searching unit 232 searches the storing unit 238 for personal information that corresponds to the media ID received by the receiving unit 231.

The file editing unit 235 refers to the corresponding personal information and generates a service file by extracting each file material, which corresponds to the user's hobby and taste shown by the personal information, from the file material storing unit 134 and editing each extracted file material. Here, if the receiving unit 231 receives a media ID reading impossible notification instead of a media ID, the file editing unit 235 generates a service file by extracting each file that appeals to all tastes from the file material storing unit 134 and editing each extracted file material.

The personal information updating unit 236 provides the data for the personal information registration screen and updates the personal information stored in the storing unit 238 with the personal information that is decrypted by the decryption unit ~~138~~133, if the personal information searching unit 232 cannot find personal information corresponding to the media ID received by the receiving unit 231 or if the receiving unit 231 receives a personal information changing request.

The transmission unit 237 transmits a media ID transmission request, a service file generated by the file editing unit 235, and the data for the personal information registration screen that is provided by the personal information updating unit 236 if the receiving unit 231 receives a service providing request.

The storing unit 238 stores personal information of users so that the personal information of each user is associated with the media ID stored in the recording medium provided to the user.

FIG. 11 shows an example of the content of the personal information that is stored in the storing unit 238.

<Operation >

FIG. 12 is a flowchart showing the processing procedure of the information processing system of the second embodiment.

The processing procedure is briefly described below with reference to ~~this drawing~~FIG. 12.

(1) The input unit 121 of the information processing apparatus 220 receives a service providing request from the user (step S21).

(2) The transmission unit 223 of the information processing apparatus 220 transmits the service providing request received by the input unit 121 to the file server 230 (step S22).

(3) The receiving unit 231 of the file server 230 receives the service providing request from the information processing apparatus 220 (step S23).

(4) The transmission unit 237 of the file server 230 transmits a media ID transmission request to the information processing apparatus 220 (step S24).

(5) The receiving unit 225 of the information processing apparatus 220 receives the media ID transmission request from the file server 230 (step S25).

(6) The reading unit 226 reads a media ID from the secure data area 111 of the recording medium 110 according to the media ID transmission request. Here, if the recording medium 210 is not connected to the information processing apparatus 220, the reading unit 226 cannot read the media ID from the secure data area 111. Also, if the device authentication between the recording medium 210 and the information processing apparatus 220 has ended in failure, the information processing apparatus 220 is prohibited ~~to access~~from accessing the secure data area 111. ~~Therefore~~In such a case, the reading unit 226 cannot read the media ID from the secure data area 111 (step S26).

(7) The transmission unit 223 of the information processing apparatus 220 transmits the media ID read by the reading unit ~~126~~226 to the file server 230. If the reading unit 126 cannot read the media ID, the transmission unit 223 transmits a media ID reading impossible notification (step S27).

(8) The receiving unit 231 of the file server 230 receives a media ID or a media ID reading impossible notification from the transmission unit 223 (step S28).

(9) It is judged whether the receiving unit 231 has received a media ID or a media ID reading impossible notification (step S29).

(10) If the receiving unit 231 has received a media ID, the personal information searching unit 232 searches the storing unit 238 for personal information corresponding to the media ID received by the receiving unit 231 (step S30).

(11) The file editing unit 235 refers to the corresponding personal information and generates a service file by extracting each file material, which corresponds to the user's hobby and taste shown by the personal information, from the file material storing unit 134 and editing each extracted file material .(step S31).

(12) If the receiving unit 231 has received a media ID reading impossible notification, the file editing unit 235 generates a service file by extracting each file material that appeals to all tastes from the file material storing unit 134 and editing each extracted file material (step S32).

(13) The transmission unit 237 transmits the service file that is generated by the file editing unit 235 (step S33).

(14) The receiving unit 225 of the information processing apparatus 220 receives the service file from the file server 230, and the display unit 127 display a service screen for the user according to the received service file (step S34).

As described above, in the information processing system of the second embodiment, a media ID is stored in a transportable recording medium. A file server receives the media ID that is read by an information processing apparatus, searches for personal information corresponding to the received media ID, and customizes a requested service according to the corresponding personal information. To use an information processing apparatus, each user needs to connect a transportable recording medium, which is uniquely assigned to the user, to the information processing apparatus. This allows the file server to correctly handle personal information of each user.

It should be noted here that each embodiment may be achieved by software. Also, the software may be stored in a computer-readable recording medium, such as a CD-ROM. Like the service providing apparatus, the computer-readable recording medium becomes the subject of production, use, transfer, lease, import, or an offer of transfer or lease.

INDUSTRIAL USE POSSIBILITY

The present invention is applicable to data communication between a user's apparatus and another apparatus, such as the access from an Internet terminal to a Web site. By uniquely providing recording media of the present invention to users, the users are in a one-to-one correspondence with the recording media even if the users are not in a one-to-one correspondence with terminals. Therefore, when a user browses a Web site, personal information of the user is correctly obtained from the user's recording medium. Also, even after replacing an old terminal with a new one, the user can continuously receive the same service by simply connecting the user's recording medium to the new terminal. This facilitates the handling of personal information of the user.

Also, a Web site does not specify a user without a recording medium being connected to a terminal. Therefore, the security of personal information is enhanced without difficulty by managing the recording media provided to users.

Further, the transportable recording medium of the present invention may store cookie information that is obtained through an Internet browser. This reduces the possibility that the cookie information may be maliciously read, causing a user's privacy to be violated or making the user a victim of cyber fraud.

ABSTRACT ~~OF THE DISCLOSURE~~

A transportable recording medium~~, such as a memory card,~~ includes an area for storing encrypted cookie information~~, such as user information, that has been encrypted using a public key obtained under a public key cryptosystem. This makes it easy to use the~~ The same cookie information is thus easy to use in different terminals and ~~has~~ the cookie information~~, which has conventionally been unique to respective terminals,~~ becomes unique to respective users instead of respective terminals. A ~~web~~ Web site reads the encrypted cookie information, decrypts the encrypted cookie information using a secret key stored in the Web site, customizes a requested service according to the decrypted cookie information, and provides the customized service to a terminal. If the Web site stores non-encrypted user information ~~that is not encrypted~~, the recording medium stores a media identification. The Web site stores the user information so that the user information of the user assigned to the ~~reading~~ recording medium is searched for according to the media identification. The Web site reads the media identification from the recording medium, searches for user information corresponding to the media identification, and customizes a requested service according to the ~~corresponding~~ user information.